~~SECRET~~

LOGGED
21 FEB 1986

# ROUTING AND RECORD SHEET

SUBJECT: (Optional)
Senate Select Committee on Intelligence Report concerning Information Security

25X1 FROM
25X1 Director of Information Services
1206 Ames Building

EXTENSION

NO. OIS*081*86

DATE 21 February 1986

| TO: (Officer designation, room number, and building) | DATE RECEIVED | DATE FORWARDED | OFFICER'S INITIALS | COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.) |
|---|---|---|---|---|
| 1. EO/DDA 7D18 Hqs | 25 FEB 1986 | | EDM | Ed, 10-10 |
| 2. ADDA | 25 FEB 1986 | | | Attached are OIS comments on the SSCI's proposed changes to the information security system. |
| 25X1 3. DDA | 25 FEB | | | [redacted] is on an interagency task force charged with preparing a report to be submitted by the President to the SSCI and HPSCI on counter-intelligence and counter-measures programs. OIS was asked to comment on the portion that concerns information security. |
| 4. DA/IRO | 28 FEB 1986 | | | I believe you should be aware of this matter. The recommendations pertaining to information security show a serious disregard or ignorance of the DCI's special authorities. |
| 5. DA/PLANS | | | | |
| 6. | | | | |
| 7. DDA REG. | | | | |
| 8. | | | | |
| 25X1 9. | | | | [redacted] |
| 10. | | | | |
| 11. | | | | |
| 12. | | | | |
| 13. | | | | UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENT B |
| 14. | | | | |
| 15. | | | | |

FORM 1-79 610 USE PREVIOUS EDITIONS

~~SECRET~~

~~INTERNAL USE ONLY~~

OIS*081*86
21 FEB 1986

Memorandum for: Director of Security

STAT From: [redacted]
Director of Information Services

Subject: Draft Senate Select Committee on Intelligence Report Concerning Information Security

1. We appreciate the opportunity to review and comment on the recommendations of the Senate Select Committee on Intelligence's (SSCI) report concerning information security. We regret that more time was not allowed for the review given the importance and complexity of some of the issues that are raised. Because of the limited time available, our comments have not been coordinated with other Agency components having an interest in these matters. Consequently the views that follow, with the exception of those that concern Recommendation No. 23, represent only the views of this Office.

2. Recommendation No. 23 of the SSCI report recommends implementation of the thirteen Information Security Oversight Office (ISOO) initiatives. An official Agency position on each of the thirteen initiatives was reached after consultation and coordination with the Office of Security, Office of General Counsel and the DCI Security Committee. The Agency opposed four of the initiatives, three concerning overclassification of information and one suggesting the revision of existing guidelines on investigations of unauthorized disclosures. We either agreed with or had no objection to the remaining nine initiatives. Attached at Tab A is a summary of the Agency position vis-a-vis the ISOO proposals.

3. Our position and comments concerning recommendations nos. 24 through 29 are:

Recommendation No. 24
Consider simplifying the classification system by establishing two levels, eliminating the current Confidential classification.

OIS Position: We oppose this proposal. It undermines the authority of the DCI to protect intelligence sources and methods. The proposed two-tier system restricts classification to the Secret level based on "substantial harm to identifiable national security interests." That implies that a "smaller" amount of harm is acceptable.

~~INTERNAL USE ONLY~~

It is not clear at what point a flow of less harmful information becomes "substantially harmful". It would be an open invitation to judicial second-guessing of the Executive Branch on matters of national security. Moreover, the second level of classification adopts a different scale on which to judge classifiability, i.e., "risk of compromise" as against "substantial damage." One concerns probability, the other a measured occurrence. It is not clear whether one is supposed to be a more exclusive or limited version of the other.

The elimination of Confidential as a classification level will not have the desired effect of eliminating or even lessening the overclassification of information. We believe it could have the opposite effect. Classifiers concerned about protecting sensitive information are likely to classify as Secret that which they would have previously classified as Confidential. This, in turn, would tend to further impede the flow of information. Finally, there appears to be no provision made for Top Secret collateral information in this new arrangement. There is a substantial body of material which, if compromised, could cause grave harm to national security but does not warrant compartmentation.

Recommendation No. 25

By Executive order, require each agency to establish procedures governing authorized disclosure of classified information to the news media, including background disclosures of information that remains classified. Such procedures should require records for accountability, consultation with originating agencies, and designation of officials authorized to disclose classified information to the media.

OIS Position: OIS endorses the establishment of procedures that would help to stem the flow of classified information to the media. Before we can make meaningful comments on this proposal, we would need considerably more information than what has been provided here. I note that on page 40 of the SSCI report, mention is made of a DCI recommendation that the NSC review "procedures for authorized contacts with the media throughout the executive branch to lessen opportunities for leaks." Obviously, "authorized contacts with the media" and "authorized disclosure of classified information" are very different. The authorized disclosure of classified information could undermine the integrity of the Secrecy Agreement.

Recommendation No. 26

Modify Executive Order 12356 to place more controls on special access programs and to give the ISSO Director greater authority to oversee such programs. Conduct a comprehensive, one-time review

and revalidation of all existing special access programs and associated "carve out" contracts with an independent assessment by the ISOO Director.

OIS Position: OIS opposes this recommendation. The DCI has statutory responsibility and authority to protect intelligence sources or methods. This authority includes special access programs pertaining to intelligence activities or intelligence sources or methods. The insertion of the D/ISOO into this process undermines the DCI's special authorities and should not be permitted. If a re-examination of special access programs is necessary, it should be undertaken as a DCI initiative.

Recommendation No. 27

Expand ISOO's staff to include a permanent inspection element. ISOO should work with DIS to implement improved training courses on information security and classification management. ISOO and the DCI should also reassess special markings with a view to simplification. ISOO should ensure that agencies pinpoint responsibility for determining need-to-know access.

OIS Position: There are three separate recommendations contained in Recommendation No. 27. We have no comment to make on the size of ISSO or its interface with DIS. The Director, ISOO is in the best position to determine his staffing needs, as well as the extent of his relationship with DIS. Concerning the recommendation that "ISOO and the DCI" reassess special markings with a view to simplification, the DCI has statutory responsibility for all aspects of special access programs having to do with intelligence sources and methods. The DCI's authority in this area should not be diminished by sharing responsibility with the Director, ISOO. If a reassessment is required, it should be done under the DCI's authority.

Recommendation No. 28

Postpone consideration of new criminal penalities for unauthorized disclosure until after the appeals in the Morison case. Continue internal agency and FBI investigations for purposes of administrative discipline or prosecution, including use of voluntary polygraph examinations under criminal investigative procedures.

OIS Position: We urge the consideration of a mandatory minimum penalty for individuals found to have made an unauthorized disclosure of classified information. We do not agree that a postponement of this issue is in the best interests of national security.

Recommendation No. 29
Review the Stilwell Commission proposals on managing and controlling classified information for government-wide implementation as part of the National Strategic Security Program.

OIS position: The Stilwell Report is a report to the Secretary of Defense by a DoD Commission and reviewed only DoD security policies and practices. Careful and detailed study would be required in order to comment on the merit of the DCI adopting either some or any of the recommendations.

4. We found a number of weaknesses in this report. It makes recommendations for improving information security without providing evidence of how that improvement will take place. In addition, the proposal to reduce the levels of classification to two, appears to be founded on contradictory assumptions. One, that too much information has been classified, the other that too much information has been underclassified. The proposed single remedy for both flaws is not a remedy.

5. The most serious aspect of this report, however, is its disregard of the DCI's statutory authority. Adoption of recommendation nos. 24, 26, or 27 would be a serious erosion of the DCI's special authorities.

6. In view of the seriousness of these issues, I suggest that the views of the Office of General Counsel and the Chairman, DCI Security Committee be sought before adoption of these recommendations gathers additional momentum. Please contact

STAT [redacted] if you have any questions regarding our comments.

STAT [redacted]

Attachment

Distribution:

OIS/IRMD/IMB/EME 19 February86

Orig - Addressee w/attachment
1 - EO/DDA w/attachment
1 - C/Administrative Law Division,OGC w/attachment
1 - C/DCI Security Committee w/attachment
1 - OS C/P&PG w/attachments
1 - D/OIS chrono w/o att
1 - IRMD chrono w/o att
1 - IMB chrono w/o att
1 - IMB Subject file w/attachment
1 - IMB Subject file CR:(ISOO Initiatives)
1 - EME w/attachment

A

Sanitized Copy Approved for Release 2011/05/05 : CIA-RDP88G01332R000200180012-8

## SUMMARY

Initiative No. 1 (Overclassification/Unnecessary Classification.).

That ISOO issue a directive on security education that includes the establishment of minimum requirements for mandatory training of classifiers of original and derivative classification decisions and the use of classification guides.

Agency Position:
We are opposed to ISOO setting standards, minimum or otherwise, for the conduct of this Agency's training and education programs. We are in compliance with EO 12356 and the current ISOO Implementing Directive which requires agencies that create and handle classified information to conduct security education. More information is needed as to what the minimum training requirements might be but to require senior agency officials to take time away from their duties to attend mandatory training is unrealistic.

Agency Resources:
Possibly one full time person. Difficult to predict without specific information concerning the extent of the training requirements. Additional administrative burden is created by the requirement to certify the training.

Initiative No. 2 (Overclassification/Unnecessary Classification).

That ISOO issue a directive on agency self-inspections that establishes minimum criteria for internal oversight, including a requirement that each agency routinely sample its classified product.

Agency Position:
We are opposed to ISOO setting standards and criteria for internal agency inspections. We are in favor of self-inspections and routine sampling of classified information.

CIA Resources:
Self-inspections and samplings of classified documents may require one additional person, depending on required frequency and the extent of the reporting requirements.

Initiative No. 3 (Overclassification/Unnecessary Classification).

That the President amend E.O. 12356 and that ISOO amend Directive No. 1 to (i) require employees to report instances of improper classification and (ii) require that agencies provide an effective means for employees to challenge classification decision free from the fear of retaliation.

Agency Position:
Opposed. Adoption of this initiative is impractical and a waste of resources. To "require" all federal employees to challenge classification decisions invites nuisance challenges rather than bona fide challenges. An individual who feels a document is improperly classified or overclassified should discuss the matter with the originator of the document. Failing internal resolution differences, Executive Order 12356, Sec 5.2, (b) (6) provides that the Director, ISOO shall consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program. This procedure has been used successfully in the past by individuals questioning the classification of documents. The D/ISOO has not presented any compelling reasons as to why it should be changed.

Agency Resources:
Impossible to judge the number of challenges this agency might draw on widely disseminated intelligence publications. The administrative processing of challenges would certainly require some additional resources but the amount will depend on where the responsibility would be assigned.

Initiative No. 4 (Overdistribution of Classified Information).

That the President issue a statement to agency heads that addresses, among other problem areas, the overdistribution of classified information.

Agency position:
Agree.

Agency Resources:
None.

Initiative No. 5 (Overdistribution of Classified Information).

That ISOO amend Directive No. 1 to provide that Federal agencies be required to review at least annually the automatic or routine distribution of all classified information and that originators and recipients update automatic distribution lists and verify the recipient's "need-to-know."

Agency position:
Agree. This is a CIA originated initiative and is based upon procedures already in practice in CPAS and the DO. Some tightening up and formalizing of current procedures will be required.

Agency Resources:

Very little, if any, additional resources likely to be needed.

Initiative No. 6 (Overdistribution of Classified Information.)

That ISOO amend Directive No. 1 to encourage agencies to place controls on the reproduction of all classified information, unless there is a countervailing reason to permit uncontrolled reproduction.

Agency position:
Agree.

Agency Resources:
No additional resources needed.

Initiative No. 7 (Classification Management)

That the President amend E. O. 12356 and that ISOO amend Directive No. 1 (1) to identify the management of classified information as an area requiring Agency head attention; and (ii) to require that responsibilities for managing classified material be included as critical elements in the performance rating system of civilian and military personnel who are original classifiers, security managers, or who are otherwise significantly involved in the management of classified information.

Agency position:
No objection. However, we see little merit in the proposal and see it turning into another pro forma rating.

Agency Resources:
None.

Initiative No. 8 (Classification Management).

That the Assistant to the President for National Security Affairs ask that the Office of Personnel Management review and revise the security specialist (GS-080) position series, to include proper recognition for the special skills required for the management of classified information.

Agency position:
No objection.

Agency Resources:
None.

Initiative No 9 (Classification Management).

That the President direct the Secretary of Defense to study the feasibility of expanding the capabilities of the Defense Security Institute (DSI) to provide basic training to all executive branch security personnel, either on a reimbursable or non-reimbursable basis.

Agency position:
No objection.

Agency Resources:
None.

Initiative No. 10 ("Need-to-know" Principle).

That the President issue a statement to agency heads stressing the importance of revitalizing the observance of the "need-to-know" principle. This statement would be part of the statement discussed in other initiatives.

Agency position:
Agree.

Agency Resources:
None.

Initiative No. 11 ("Need-to-know" Principle).

That the President amend E. O. 12356 to require agency heads to ensure effective internal oversight of special access programs, including periodic confirmation of their continued need.

Agency Position:
No objection. Presently EO 12356 very clearly puts the responsibility for special access programs with Agency heads.

Agency Resources:
None anticipated.

Initiative No. 12 (Unauthorized Disclosures).

That ISOO coordinate with the Security Committee (SECOM) of the Intelligence Community the development of educational materials, both classified and unclassified, addressing the damage caused by unauthorized disclosures.

Agency position:
No objection. SECOM is developing educational material on the damage caused by unauthorized disclosures. C/SECOM has indicated that he would welcome any suggestions particularly on the production of really effective unclassified educational material showing the damage done by unauthorized disclosures.

Agency Resources:
None anticipated.

Initiative No. 13 (Unauthorized Disclosures).

That the President call upon the Attorney General to revise existing guidelines on investigations of unauthorized disclosures.

Agency position:
We are opposed to having internal Agency investigative procedures dictated. In presenting this initiative, ISOO cites the lack of successful prosecutions or administrative sanctions associated with unauthorized disclosures. The lack of success in this area is not due to faulty Agency investigations.

Agency Resources:
Probably no additional resources.

B

SECRET

# ROUTING AND RECORD SHEET

SUBJECT (Optional)
Counterintelligence and Countermeasures Programs

25X1 FROM

25X1 Chief, Policy Branch/PPS
Office of Security

EXTENSION

NO.

DATE 18 February 1986

| TO (Officer designation, room number, and building) | DATE RECEIVED | DATE FORWARDED | OFFICER'S INITIALS | COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.) |
|---|---|---|---|---|
| 1. C/IRMD/OIS | 19 Feb 86 | | | An interagency task force is currently preparing a report to be submitted by the President to the SSCI and HPSCI on counterintelligence and countermeasures programs. The report deals very little with information security, per se, but has touched on the ISOO recommendations. Attached is a portion of an SSCI report. The extract deals with items on which OIS may wish to comment. The task force will use our comments on this and other materials as input or background in preparing the President's report.<br><br>Please note that we already have an Agency position on those items which are nothing more than repetition of the ISOO report. Nonetheless, you may wish to comment on recommendations 23 and 27. Your views on any other aspect of the attached are also welcome. Unfortunately, we have a very short deadline.<br><br>Please respond no later than noon, 21 February, as we must have our comments to the task force on 24 February.<br><br>[redacted] |
| 2. att. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| 6. | | | | |
| 7. | | | | |
| 8. | | | | |
| 9. | | | | |
| 10. | | | | |
| 11. | | | | |
| 12. | | | | |
| 13. | | | | |
| 14. | | | | |
| 15. | | | | |

25X1

25X1

25X1

FORM 610 EDITIONS

SECRET

B. Information Security

In December, 1985, the Committee submitted to the National Security Council a series of recommendations on information security, in response to a request for input on proposals developed by the Information Security Oversight Office (ISOO). In addition to calling for a National Strategic Security Program, as discussed above, the Committee urged immediate implementation of the ISOO proposals with strong, public endorsement of the President and the principal members of the National Security Council. The ISOO proposals would establish new information security policies for curbing overclassification and overdistribution, improving classification management, enforcing the need-to-know principle, and improving security awareness and investigations of unauthorized disclosures. The Committee recommended that senior executives and program managers be held personally responsible for effective implementation of these policies.

Although the ISOO proposals are an excellent agenda for near-term actions, the Committee made several other recommendations for long-term decisions. First, there is a fundamental problem with the classification system because of its complexity. The Committee recommended consideration of a two-level system, based essentially

on the current Secret standard and the Sensitive Compartmented Information model used in the Intelligence Community. A two-tier system offers a better chance of enforcing the need-to-know principle and reversing the natural incentives to overclassification.

The Confidential classification should be dropped, with such information either kept unclassified or protected at the Secret level. The initial decision should be whether the information requires protection in order to prevent substantial harm to identifiable national security interests.

The classification threshold should reflect a policy that classifies information only where truly necessary to maintain national security. The report on Scientific Communication and National Security, issued in 1982 by a panel of the National Academy of Sciences, warned that undue controls can "weaken both military and economic capabilities by restricting the mutually beneficial interaction of scientific investigators, inhibiting the flow of research results into military and civilian technology, and lessening the capacity of universities to train advanced researchers." The 1985 interagency report on Soviet Acquisition of Militarily Significant Western Technology reiterated the warning that restricting access to scientific data "may also inhibit the United States' own national research effort." As stated recently by former DIA Director Eugene F. Tighe, "[I]f the U.S. security system for handling classified material is to be useful, only data that are

critical to the United States' status as a political, economic and military power should be classified." The assumption should be that information is unclassified, unless there is a specific reason for maintaining secrecy.

The higher classification standard should focus on the much smaller universe of data that require special protective measures above and beyond the normal safeguards for classified information. As is the case with intelligence data designated SCI, classification at the second level should be based on a full analysis of the risks of compromise. Such analysis should ensure that special protective measures are imposed only where necessary and are not diluted by applying them too widely. Careful analysis should also provide the elements for more effective security briefings that help senior policy-makers as well as lower level employees understand the consequences of a security breach.

25X1

[redacted]

Another concern is that a higher classification threshold would make more documents accessible under the Freedom of Information Act or otherwise. However, unclassified information of a sensitive character can be marked "For Official Use Only" to maintain a policy of not releasing such materials publicly. Concern about FOIA should not dictate classification management policy, which should be geared to the most efficient protection against hostile intelligence access to truly important secrets. If specific types of unclassified, but sensitive, information require exemption from the FOIA, Congress should enact appropriate legislation as has been done for certain kinds of Defense Department technical data. This would be in keeping with the report on Scientific Communication and National Security, which called for development of specific criteria to determine

whether unclassified scientific research should be protected by means short of classification.

The other information security recommendations sent to the NSC by the Committee addressed the problem of disclosure of classified information to the news media. The Committee is especially concerned about leaks that compromise sensitive intelligence sources and methods. The Committee emphasized the ISOO recommendation that more effective, unclassified educational materials be developed to explain the damage caused by unauthorized disclosures. The more important recommendation was for new procedures for authorized disclosure of classified information to the news media.

The National Assessment of Hostile Intelligence Services Threat and U.S. Countermeasures, sent to the NSC

in May, 1985, specifically recommended "establishment of government-wide regulations governing media contacts by persons with access to sensitive intelligence." According to the National Assessment, the DCI recommended in November, 1984, that the NSC review "procedures for authorized contacts with the media throughout the executive branch to lessen opportunities for leaks." The Committee endorsed these recommendations.

The Committee recommended that the NSC confront the pervasive practice of authorized disclosure of classified information on background, without permitting attribution to the source. By Executive order, the President should require each agency to establish procedures to be followed whenever an official authorizes disclosure of classified information to the news media or other public forum. The procedures should apply not only to formal statements for attribution, but also to disclosures on background. They should require that a decision be made to declassify the exposed information or that a record be maintained for purposes of accountability when authority is exercised or granted to disclose information that remains classified. The procedures should require consultation with the agency that originated the information and written designation of the officials in each agency who are authorized to communicate classified information to the media, either in person or through an authorized representative.

Some Executive branch officials oppose such procedures as likely to open the floodgates for "authorized leaks." Others want strict enforcement of a policy that any classified information disclosed to the media be officially declassified. The Committee strongly encourages adherence to a policy that officials speak on the record to the maximum extent. Nevertheless, there may well be valid reasons for retaining a background briefing's classified character. Any serious effort to address the problem of leaks must face the realities of press-government relations. More leak investigations may accomplish little, moreover, so long as authorized background disclosures continue to divert investigators from cases in which administrative discipline, dismissal, or legal action is possible. Policies that ignore "authorized leaks" simply reinforce the climate of cynicism that has fostered disrespect for security.

In addition to the recommendations submitted to the NSC in December, 1985, the Committee has several other information security recommendations. Many proposals of the Stilwell Commission on managing and controlling classified information should be considered government-wide. These include recommendations to:

- Require, rather than simply permit, challenges to classifications believed to be improper.
- Require a higher minimum degree of accountability for Secret documents.
- Impose better controls over reproduction equipment used to copy classified information.
- Initiate long-term action to develop technical or mechanical controls over unauthorized reproduction.
- Reduce unnecessary retention and storage of classified documents.
- Prohibit employees from working alone in areas where Top Secret or similarly sensitive materials are in use or stored.

The Stilwell Commission recommendations on special access programs and on National Disclosure Policy for transfers of classified information to foreign governments are particularly important.

The proliferation of special access programs is testimony to the failure of the current security system. ISOO Director Steven Garfinkel testified that "a number of these programs are probably unnecessary," and the Stilwell Commission reported that some actually afford less security protection than ordinary classification requirements. The Stilwell Commission's proposed policies, standards, and controls for special access programs should be adopted government-wide. Moreover, Executive Order 12356 on National Security Information should be modified to place

more controls on the establishment of special access programs and to give the ISOO Director greater authority to conduct oversight and ensure accountability of special access programs. There should be a comprehensive, one-time review and revalidation of all existing special access programs and associated "carve out" contracts, with each department and agency reporting the results to the ISOO Director who should make an independent assessment for the NSC.

The Committee believes ISOO has made a valuable contribution to better information security, but its small size (10 professionals) unduly limits its ability to conduct oversight inspections and other in-depth evaluations. ISOO's staff should be expanded to include a permanent element to inspect agency practices at all levels of command and management. While ISOO cannot replace internal

with a view to simplifying the special marking systems, including practices in the SCI field.

Special markings help to enforce need-to-know restrictions by warning a reader what accesses are required to read a document. Equally important, however, is a clear assignment of responsibility for determining whether someone has a need for access to information about a particular program. ISOO should review current directives and regulations to ensure that such responsibilities are pinpointed and that compliance is audited regularly.

Finally, the Committee does not believe that legislation to enhance criminal enforcement remedies for unauthorized disclosure of classified information would be appropriate this year. After completion of the appeals in the Morison case, a reassessment by both Congress and the Executive branch might be in order. The Committee does, however, support continued investigation of unauthorized disclosures within agencies and by the FBI for purposes of administrative discipline as well as criminal prosecution. Polygraph examinations should also continue to be used in leak investigations on a voluntary basis in accordance with procedures followed in other types of criminal investigations.

inspections, it should do more to ensure the effectiveness of agency inspections by sampling on an aperiodic basis. ISOO should also work closely with the Defense Security Institute to implement the government-wide policy (proposed by ISOO) requiring seminars and training courses for all levels of commanders and managers, in government and industry, to understand information security policy and procedures, especially classification management.*

An informal query of government and industrial managers by Committee staff tends to validate the claim that managers are often deficient in their knowledge of classification management requirements and procedures. This is a particular problem in the Sensitive Compartmented Information area, where special markings proliferate. The proliferation of classified documents and the need for greater security has spawned an entire dictionary of special classification markings and control systems. The rise of these special markings and control systems has tended to generate a false sense of security and in the process to confuse those who do not fully understand their meanings. It is not unusual to see documents with a classification, several control signature designations, and four or five special markings each telling the reader to be very careful. ISOO should undertake a thorough reassessment of these practices

* See also recommendation __ for a West Coast annex to the Defense Security Institute.

RECOMMENDATIONS:

(23) Immediately implement the ISOO proposals with strong public endorsement of the President and the principal members of the National Security Council.

(24) Consider simplifying the classification system by establishing two levels, eliminating the current Confidential classification.

(25) By Executive order, require each agency to establish procedures governing authorized disclosure of classified information to the news media, including background disclosures of information that remains classified. Such procedures should require records for accountability, consultation with originating agencies, and designation of officials authorized to disclose classified information to the media.

(26) Modify Executive Order 12356 to place more controls on special access programs and to give the ISOO Director greater authority to oversee such programs. Conduct a comprehensive, one-time review and revalidation of all existing special access programs and associated "carve out" contracts, with an independent assessment by the ISOO Director.

(27) Expand ISOO's staff to include a permanent inspection element. ISOO should work with DIS to implement improved training courses on information security and classification management. ISOO and the DCI should also

reassess special markings with a view to simplification. ISOO should ensure that agencies pinpoint responsibility for determining need-to-know access.

(28) Postpone consideration of new criminal penalties for unauthorized disclosure until after the appeals in the Morison case. Continue internal agency and FBI investigations for purposes of administrative discipline or prosecution, including use of voluntary polygraph examinations under criminal investigative procedures.

(29) Review the Stilwell Commission proposals on managing and controlling classified information for government-wide implementation as part of the National Strategic Security Program.